UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/789,809	02/27/2004	Trevor W. Freeman	MS1-1747US	5655

22801   7590   09/04/2008

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER
KAPLAN, BENJAMIN A

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
09/04/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
	10/789,809	FREEMAN ET AL.
Office Action Summary	Examiner	Art Unit	
	BENJAMIN A. KAPLAN	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _05 May 2008_.
2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _1-5,7-13 and 15-34_ is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) _1-5,7-13 and 15-34_ is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on _27 February 2004_ is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a) ☐ All   b) ☐ Some * c) ☐ None of:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____.
      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _8/26/08_.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1.   This Office action is in regards to the most recent papers filed on 05 May 2008.

2.   Claims 1-5, 7-13 & 15-34 are pending.

3.   Claims 6 & 14 are canceled.

4.   Claims 1, 9, 16, 23, 30 & 34 are amended.

5.   Claims 1-5, 7-13 & 15-34 are rejected.

Response to Amendments

6.   The rejection of Claim 16 under 35 USC § 112 is withdrawn.

7.   The previous rejection of Claims 1-5, 7-8, 16-22 & 30-34 under 35 USC § 101 is

withdrawn.

8.   Previous rejections made under 35 USC § 102 and 35 USC § 103 are withdrawn.

Claim Rejections - 35 USC § 101

9.   35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 23-29 are rejected under 35 U.S.C. 101 because the claimed invention is

directed to non-statutory subject matter.

Claims 23-29 are non-statutory because a protocol is a technique of doing

something which is an abstract idea.

Applicant may consider substituting "A method" for "A protocol".

Claim Rejections - 35 USC § 102

10.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11.   Claim 1-5, 7, 9-13, 16-21, 23-28 & 30-33 rejected under 35 U.S.C. 102(b) as

being anticipated by United States Patent Application Publication No. US 2001/0020228

A1 (Cantu et al.).

Cantu et al incorporates the Handbook of Applied Cryptography (Handbook)

(Cantu et al., Paragraph [0054], Lines 12-21 "Public key algorithms include the

Rivest, Shamir, and Adleman (RSA) algorithm, or may include any public key encryption

algorithm known in the art, such as Diffie and Hellman. Further details of public key

encryption is described in the publication "An Overview of the PKCS Standards," RSA

Laboratories Technical Note, by Burton S. Kaliski, Jr. (1993) and "Handbook of Applied

Cryptography," by Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone

(1996), which publications are incorporated herein by reference in their entirety.").

12.   Claim 1-3, 7, 9-11, 16-19, 23-26, 30 & 31 are rejected under 35 U.S.C. 102(b) as

being anticipated by United States Patent Application Publication No. US 2001/0020228

A1 (Cantu et al.). Interpreting the claims as establishing symmetric keys.

As per Claim 1: Cantu et al. teaches: **An out-of-band method for asynchronously establishing a secure association with a remote node, comprising:**

- generating a local public value and a local private value on at least one node

(Handbook, Chapter 12, Page 516, Section 12.47, "

12.47 Protocol Diffie-Hellman key agreement (basic version)

SUMMARY: A and B each send the other one message over an open channel.
RESULT: shared secret K known to both parties A and B.

1. *One-time setup.* An appropriate prime p and generator α of $\mathbb{Z}_p^*$ $(2 \leq \alpha \leq p - 2)$ are selected and published.

2. *Protocol messages.*

$$A \rightarrow B : \alpha^x \bmod p \quad (1)$$
$$A \leftarrow B : \alpha^y \bmod p \quad (2)$$

3. *Protocol actions.* Perform the following steps each time a shared key is required.

   (a) A chooses a random secret x, $1 \leq x \leq p - 2$, and sends B message (1).

   (b) B chooses a random secret y, $1 \leq y \leq p - 2$, and sends A message (2).

   (c) B receives α^x and computes the shared key as $K = (\alpha^x)^y \bmod p$.

   (d) A receives α^y and computes the shared key as $K = (\alpha^y)^x \bmod p$.

").

Party A is one node, α or p are the public value, and x is the private value.

- storing the public value for configuration of the secure association on an out-of-band computer-readable storage medium wherein the stored public value is not used for authentication

- transporting the out-of-band computer-readable storage medium to the other node

- receiving the public value from the other node via the out-of-band computer-readable storage medium

(Cantu et al., Paragraph [0107], "In the described implementations of FIGS. 8 and 9, the parties exchanged public keys using computer diskettes or secure e -mail. However, alternative secure techniques can be used by the parties to exchange keys, whether or not such exchange occurs as part of a transaction related to the preexisting relationships 400, 402, 404 or some unrelated exchange.").

Exchanging Keys using computer diskettes stores a value on the diskette (computer-readable storage medium) at one node and transports the diskette to give the value to the other node.

- generating a secret value using the local private value in combination with the public value received from the other node; wherein the receiving is asynchronous to the generating

(Handbook, Chapter 12, Page 516, Section 12.47, "

12.47 Protocol Diffie-Hellman key agreement (basic version)

SUMMARY: A and B each send the other one message over an open channel.

RESULT: shared secret K known to both parties A and B.

1. *One-time setup*. An appropriate prime p and generator α of $\mathbb{Z}_p^*$ ($2 \leq \alpha \leq p - 2$) are selected and published.

2. *Protocol messages*.

$$A \rightarrow B : \alpha^x \bmod p \quad (1)$$
$$A \leftarrow B : \alpha^y \bmod p \quad (2)$$

3. *Protocol actions*. Perform the following steps each time a shared key is required.

   (a) A chooses a random secret x, $1 \leq x \leq p - 2$, and sends B message (1).

   (b) B chooses a random secret y, $1 \leq y \leq p - 2$, and sends A message (2).

   (c) B receives α^x and computes the shared key as $K = (\alpha^x)^y \bmod p$.

   (d) A receives α^y and computes the shared key as $K = (\alpha^y)^x \bmod p$.

”).

Protocol actions, Step (d); Shared key K is the generated secret value.

As per Claim 2: The rejection of claim 1 is incorporated and further Cantu et al. teaches:

- the method is performed on both of a pair of nodes, and wherein further the secret values generated at both of the nodes are symmetric

(Handbook, Chapter 12, Page 516, Section 12.47, "

12.47 Protocol Diffie-Hellman key agreement (basic version)

SUMMARY: A and B each send the other one message over an open channel.

RESULT: shared secret K known to both parties A and B.

1. *One-time setup.* An appropriate prime p and generator α of $\mathbb{Z}_p^*$ ($2 \le \alpha \le p - 2$) are selected and published.

2. *Protocol messages.*

$$A \to B : \alpha^x \bmod p \quad (1)$$
$$A \leftarrow B : \alpha^y \bmod p \quad (2)$$

3. *Protocol actions.* Perform the following steps each time a shared key is required.

   (a) A chooses a random secret x, $1 \le x \le p - 2$, and sends B message (1).

   (b) B chooses a random secret y, $1 \le y \le p - 2$, and sends A message (2).

   (c) B receives α^x and computes the shared key as $K = (\alpha^x)^y \bmod p$.

   (d) A receives α^y and computes the shared key as $K = (\alpha^y)^x \bmod p$.

").

The method is performed at both nodes. Both nodes generate the secret value shared key K.

As per Claim 3: The rejection of claim 2 is incorporated and further a performing a Diffie-Hellman key agreement as discussed in claims 1 and 2 is a Diffie-Hellman computation.

As per Claim 7: The rejection of claim 1 is incorporated and further Cantu et al. teaches:

- the receiving of the public value from the other node via an out-of-band mechanism includes downloading the public value from an external device

(Cantu et al., Paragraph [0107], "In the described implementations of FIGS. 8 and 9, the parties exchanged public keys using computer diskettes or secure e -mail. However, alternative secure techniques can be used by the parties to exchange keys, whether or not such exchange occurs as part of a transaction related to the preexisting relationships 400, 402, 404 or some unrelated exchange.").

A computer diskette is an external device.

As per Claim 9: Claim 9 is substantially the method claim of claim 1 as a computer readable storage medium and is rejected under substantially the same reasoning as set forth in the rejection of claim 1.

As per Claim 10: The rejection of claim 9 is incorporated and further:

Claim 10 is substantially the method claim of claim 2 as a computer readable medium and is rejected under substantially the same reasoning as set forth in the rejection of claim 2.

As per Claim 11: The rejection of claim 9 is incorporated and further:

Claim 11 is substantially the method claim of claim 3 as a computer readable medium and is rejected under substantially the same reasoning as set forth in the rejection of claim 3.

As per Claim 16: Claim 16 is substantially the method claim of claim 1 as an apparatus and is rejected under substantially the same reasoning as set forth in the rejection of claim 1.

As per Claim 17: The rejection of claim 16 is incorporated and further:

Claim 17 is substantially the method claim of claim 2 as an apparatus and is rejected under substantially the same reasoning as set forth in the rejection of claim 2.

As per Claim 18: The rejection of claim 16 is incorporated and further in accordance with Cantu et al.'s method the other node may be a server.

As per Claim 19: The rejection of claim 16 is incorporated and further:

Claim 19 is substantially the method claim of claim 3 as an apparatus and is rejected under substantially the same reasoning as set forth in the rejection of claim 3.

As per Claim 23: Claim 23 is substantially the method claim of claim 1 as a protocol and is rejected under substantially the same reasoning as set forth in the rejection of claim 1.

As per Claim 24: The rejection of claim 23 is incorporated and further:

Claim 24 is substantially the method claim of claim 2 as a protocol and is rejected under substantially the same reasoning as set forth in the rejection of claim 2.

As per Claim 25: The rejection of claim 24 is incorporated and further:

Claim 25 is substantially the method claim of claim 3 as a protocol and is rejected under substantially the same reasoning as set forth in the rejection of claim 3.

As per Claim 26: The rejection of claim 24 is incorporated and further as both parties end up with shared key K in the Diffie-Hellman method the shared secret is symmetrical.

As per Claim 30: Claim 30 is substantially the method claim of claim 1 as an apparatus and is rejected under substantially the same reasoning as set forth in the rejection of claim 1.

As per Claim 31: The rejection of claim 30 is incorporated and further:

Claim 31 is substantially the method claim of claim 3 as an apparatus and is rejected under substantially the same reasoning as set forth in the rejection of claim 3.

13.   Claim 1, 4, 5, 7, 9, 12, 13, 16, 18, 20, 21, 23, 27, 28, 30, 32 & 33 are rejected under 35 U.S.C. 102(b) as being anticipated by United States Patent Application Publication No. US 2001/0020228 A1 (Cantu et al.). Interpreting the claims as first establishing asymmetric keys.

As per Claim 1: Cantu et al. teaches: **An out-of-band method for asynchronously**

establishing a secure association with a remote node, comprising:

- generating a local public value and a local private value on at least one node

(Handbook, Chapter 8, Page 286, Section 8.1 - 8.2, "

8.1 Algorithm Key generation for RSA public-key encryption

SUMMARY: each entity creates an RSA public key and a corresponding private key.
Each entity A should do the following:

1. Generate two large random (and distinct) primes p and q, each roughly the same size.
2. Compute $n = pq$ and $\phi = (p - 1)(q - 1)$. (See Note 8.5.)
3. Select a random integer e, $1 < e < \phi$, such that $\gcd(e, \phi) = 1$.
4. Use the extended Euclidean algorithm (Algorithm 2.107) to compute the unique integer d, $1 < d < \phi$, such that $ed \equiv 1 \pmod{\phi}$.
5. A's public key is (n, e); A's private key is d.

8.2 Definition The integers e and d in RSA key generation are called the *encryption exponent* and the *decryption exponent*, respectively, while n is called the *modulus*.

").

Public key (n,e) is the public value, Private key d is the private value.

- storing the public value for configuration of the secure association on an out-of-

band computer-readable storage medium wherein the stored public value is not

used for authentication

- transporting the out-of-band computer-readable storage medium to the other

node

- receiving the public value from the other node via the out-of-band computer-readable storage medium

(Cantu et al., Paragraph [0107], "In the described implementations of FIGS. 8 and 9, the parties exchanged public keys using computer diskettes or secure e -mail. However, alternative secure techniques can be used by the parties to exchange keys, whether or not such exchange occurs as part of a transaction related to the preexisting relationships 400, 402, 404 or some unrelated exchange.").

Exchanging Keys using computer diskettes stores a value on the diskette (computer-readable storage medium) at one node and transports the diskette to give the value to the other node.

(Handbook, Chapter 8, Page 286, Section 8.3, "

8.3 Algorithm RSA public-key encryption

SUMMARY: B encrypts a message m for A, which A decrypts.
1. *Encryption.* B should do the following:
    (a) Obtain A's authentic public key (n, e).
    (b) Represent the message as an integer m in the interval $[0, n-1]$.
    (c) Compute $c = m^e \bmod n$ (e.g., using Algorithm 2.143).
    (d) Send the ciphertext c to A.
2. *Decryption.* To recover plaintext m from c, A should do the following:
    (a) Use the private key d to recover $m = c^d \bmod n$.

").

The obtained public key is the received public value.

- generating a secret value using the local private value in combination with the public value received from the other node; wherein the receiving is asynchronous to the generating

(Handbook, Chapter 8, Page 290, Section 8.2.3, "

8.2.3 RSA encryption in practice

There are numerous ways of speeding up RSA encryption and decryption in software and hardware implementations. Some of these techniques are covered in Chapter 14, including fast modular multiplication (§14.3), fast modular exponentiation (§14.6), and the use of the Chinese remainder theorem for faster decryption (Note 14.75). Even with these improvements, RSA encryption/decryption is substantially slower than the commonly used symmetric-key encryption algorithms such as DES (Chapter 7). In practice, RSA encryption is most commonly used for the transport of symmetric-key encryption algorithm keys and for the encryption of small data items.

The RSA cryptosystem has been patented in the U.S. and Canada. Several standards organizations have written, or are in the process of writing, standards that address the use of the RSA cryptosystem for encryption, digital signatures, and key establishment. For discussion of patent and standards issues related to RSA, see Chapter 15.

").

The secret value is the symmetric-key established though the use of the RSA public and private keys.

As per Claim 4: The rejection of claim 1 is incorporated and further Cantu et al. teaches:

- retaining the secret value locally

It is inherently necessary to retain the secret value in order to take any further action using it or based on it.

- **protecting the secret value using the public value received from the other node**

- **transmitting the protected secret value to the other node**

(Handbook, Chapter 8, Page 286, Section 8.3, "

8.3 Algorithm RSA public-key encryption

SUMMARY: B encrypts a message m for A, which A decrypts.

1. *Encryption.* B should do the following:

   (a) Obtain A's authentic public key (n, e).

   (b) Represent the message as an integer m in the interval $[0, n-1]$.

   (c) Compute $c = m^e \bmod n$ (e.g., using Algorithm 2.143).

   (d) Send the ciphertext c to A.

2. *Decryption.* To recover plaintext m from c, A should do the following:

   (a) Use the private key d to recover $m = c^d \bmod n$.

").

(Handbook, Chapter 8, Page 290, Section 8.2.3, "

8.2.3 RSA encryption in practice

There are numerous ways of speeding up RSA encryption and decryption in software and hardware implementations. Some of these techniques are covered in Chapter 14, including fast modular multiplication (§14.3), fast modular exponentiation (§14.6), and the use of the Chinese remainder theorem for faster decryption (Note 14.75). Even with these improvements, RSA encryption/decryption is substantially slower than the commonly used symmetric-key encryption algorithms such as DES (Chapter 7). In practice, RSA encryption is most commonly used for the transport of symmetric-key encryption algorithm keys and for the encryption of small data items.

The RSA cryptosystem has been patented in the U.S. and Canada. Several standards organizations have written, or are in the process of writing, standards that address the use of the RSA cryptosystem for encryption, digital signatures, and key establishment. For discussion of patent and standards issues related to RSA, see Chapter 15.

").

In the practice of using RSA encryption for transporting the secret value (symmetric-key); The symmetric-key would be the contents of message m protected by the received public key sent as the protected value c.

- via an out-of-band mechanism

(Cantu et al., Paragraph [0107], "In the described implementations of FIGS. 8 and 9, the parties exchanged public keys using computer diskettes or secure e -mail. However, alternative secure techniques can be used by the parties to exchange keys, whether or not such exchange occurs as part of a transaction related to the preexisting relationships 400, 402, 404 or some unrelated exchange.").

A computer diskettes is an out-of-band mechanism.

As per Claim 5: The rejection of claim 4 is incorporated and further a performing RSA encryption practices as discussed in claims 1 and 4 is a Rivest-Shamir-Adleman (RSA) computation.

As per Claim 7: The rejection of claim 1 is incorporated and further Cantu et al. teaches:

- the receiving of the public value from the other node via an out-of-band mechanism includes downloading the public value from an external device

(Cantu et al., Paragraph [0107], "In the described implementations of FIGS. 8 and 9, the parties exchanged public keys using computer diskettes or secure e -mail. However, alternative secure techniques can be used by the parties to exchange keys, whether or not such exchange occurs as part of a transaction related to the preexisting relationships 400, 402, 404 or some unrelated exchange.").

A computer diskette is an external device.

As per Claim 9: Claim 9 is substantially the method claim of claim 1 as a computer readable medium and is rejected under substantially the same reasoning as set forth in the rejection of claim 1.

As per Claim 12: The rejection of claim 9 is incorporated and further:

Claim 12 is substantially the method claim of claim 4 as a computer readable medium and is rejected under substantially the same reasoning as set forth in the rejection of claim 4.

As per Claim 13: The rejection of claim 12 is incorporated and further:

Claim 13 is substantially the method claim of claim 5 as a computer readable medium and is rejected under substantially the same reasoning as set forth in the rejection of claim 5.

As per Claim 16: Claim 16 is substantially the method claim of claim 1 as an apparatus and is rejected under substantially the same reasoning as set forth in the rejection of claim 1.

As per Claim 18: The rejection of claim 16 is incorporated and further in accordance with Cantu et al.'s method the other node may be a server.

As per Claim 20: The rejection of claim 16 is incorporated and further:

Claim 20 is substantially the method claim of claim 4 as a computer readable medium and is rejected under substantially the same reasoning as set forth in the rejection of claim 4.

As per Claim 21: The rejection of claim 20 is incorporated and further:

Claim 21 is substantially the method claim of claim 5 as a computer readable medium and is rejected under substantially the same reasoning as set forth in the rejection of claim 5.

As per Claim 23: Claim 23 is substantially the method claim of claim 1 as a protocol and is rejected under substantially the same reasoning as set forth in the rejection of claim 1.

As per Claim 27: The rejection of claim 23 is incorporated and further:

Claim 27 is substantially the method claim of claim 4 as a protocol and is rejected under substantially the same reasoning as set forth in the rejection of claim 4.

As per Claim 28: The rejection of claim 27 is incorporated and further:

Claim 28 is substantially the method claim of claim 5 as a protocol and is rejected under substantially the same reasoning as set forth in the rejection of claim 5.

As per Claim 30: Claim 30 is substantially the method claim of claim 1 as an apparatus with means for and is rejected under substantially the same reasoning as set forth in the rejection of claim 1. An apparatus conducting these processes inherently has a means for doing so.

As per Claim 32: The rejection of claim 30 is incorporated and further:

Claim 32 is substantially the method claim of claim 4 as an apparatus with means for and is rejected under substantially the same reasoning as set forth in the rejection of claim 4. An apparatus conducting these processes inherently has a means for doing so.

As per Claim 33: The rejection of claim 32 is incorporated and further:

Claim 33 is substantially the method claim of claim 5 as an apparatus with means for and is rejected under substantially the same reasoning as set forth in the rejection of claim 5. An apparatus conducting these processes inherently has a means for doing so.

Claim Rejections - 35 USC § 103

14.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15.   Claims 8, 15, 22, 29 & 34 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Cantu et al. In further view of Official Notice.

As per Claim 8: The rejection of either claim 7 is incorporated and further Cantu et al.

does not explicitly teach:

- the external device is any one of a personal digital assistant (PDA), flash

memory, memory stick, barcode, smart card, USB-compatible device, Bluetooth-

compatible device, and infrared-compatible device.

However the Examiner is giving Official Notice that these are all functional equivalents

of computer diskettes that were well know in the art at the time of invention was made.

It would have been obvious to one of ordinary skill in the art at the time of invention was

made to incorporate compatibility with these various mediums into Cantu et al.'s method

in order to have a variedly of redundant/faster/convenient mediums available to the

working system.

As per Claim 15: The rejection of either claim 9 is incorporated and further:

Claim 15 is substantially a restatement of the limitation of claim 8 and is rejected under substantially the same reasoning as set forth in the rejection of claim 8.

As per Claim 22: The rejection of either claim 16 is incorporated and further:

Claim 22 is substantially a restatement of the limitation of claim 8 and is rejected under substantially the same reasoning as set forth in the rejection of claim 8.

As per Claim 29: The rejection of either claim 23 is incorporated and further:

Claim 34 is substantially a restatement of the limitation of claim 8 and is rejected under substantially the same reasoning as set forth in the rejection of claim 8.

As per Claim 34: The rejection of either claim 30 is incorporated and further:

Claim 34 is substantially a restatement of the limitation of claim 8 and is rejected under substantially the same reasoning as set forth in the rejection of claim 8.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN A. KAPLAN whose telephone number is (571)270-3170. The examiner can normally be reached on 7:30 a.m. - 5:00 p.m. E.S.T..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on 571-272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Benjamin Kaplan

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139